

Dokumentationsanforderungen an Finanzunternehmen gemäß DORA

Kapitel II IKT-Risikomanagement, Abschnitt II DORA													Kapitel III DORA Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle	Kapitel IV DORA Testen der digitalen operationalen Resilienz	Kapitel V, Abschnitt I DORA Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos			
Strategien	Artikel 6 DORA IKT-Risikomanagement- rahmen <div><div>DOR-Strategie (Art. 6 Abs. 8 i.V.m. Art. 5 Abs. 2 lit. d DORA)</div><div>Geschäftsstrategie (Art. 6 Abs. 8 lit. a DORA)</div></div>	Artikel 8 DORA Identifizierung	Artikel 9 DORA Schutz und Prävention <div><div>Informations-sicherheitsleitlinie (Art. 9 Abs. 4 lit. a DORA)</div><div><div>Titel II – Kapitel I RTS RMF – Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit</div><div><div>Abschnitt 2 Richtlinien für das IKT-Risikomanagement (Art. 3 RTS RMF)</div><div><div>Abschnitt 3 Richtlinie für das Management von IKT-Assets (Art. 4 RTS RMF i.V.m. Art. 9 Abs. 2 und 4 lit. c DORA)</div><div><div>Abschnitt 4 Richtlinie für Verschlüsselung und kryptografische Kontrollen (Art. 6 und 7 RTS RMF i.V.m. Art. 9 Abs. 2 DORA)</div><div><div>Abschnitt 5 Richtlinien für das Management der IKT-Vorgänge (Betrieb) (Art. 8 RTS RMF i.V.m. Art. 9 Abs. 2 DORA)</div><div><div>Abschnitt 6 Richtlinien für das Management der Netzwerksicherheit (Art. 13 RTS RMF)</div><div><div>Abschnitt 7 Richtlinien für das IKT-Projektmanagement (inkl. IKT-Projektrisikobewertung) (Art. 15 RTS RMF)</div><div><div>Abschnitt 8 Richtlinien für die physische Sicherheit und die Sicherheit vor Umweltereignissen (Art. 18 RTS RMF)</div></div><div><div>Richtlinien für die Datensicherung (Backup) (Art. 12 Abs. 1 lit. a und Abs. 2 DORA)</div><div><div>Richtlinien für die Behandlung IKT-bezogener Vorfälle (Art. 22 und 23 RTS RMF)</div></div></div></div><div><div>Titel II – Kapitel II RTS RMF – Richtlinien für Personalpolitik und Zugangskontrolle</div><div><div>Richtlinien für Personalpolitik (Art. 19 RTS RMF)</div><div><div>Richtlinien für das Identitätsmanagement (Art. 20 RTS RMF)</div><div><div>Richtlinien im Rahmen der Kontrolle der Zugangs- und Zugriffsrechte (Art. 21 RTS RMF i.V.m. Art. 9 Abs. 4 lit. c DORA)</div></div></div></div></div></div></div></div></div></div></div></div>						Artikel 10 DORA Erkennung	Artikel 11 DORA Reaktion und Wiederherstellung <div><div>IKT-Geschäftsfortführungsleitlinie (Art. 11 DORA i.V.m. Art. 5 Abs. 2 lit. e und Art. 8 DORA, Art. 24 RTS RMF)</div><div>(Allgemeine) Geschäftsfortführungsleitlinie (inkl. BIA) (Art. 11 Abs. 1 und 5 i.V.m. Art. 5 Abs. 2 lit. e DORA)</div></div>	Artikel 12 DORA Richtlinie und Verfahren zum Backup <div>Richtlinien für die Datensicherung (Backup) (Art. 12 Abs. 1 lit. a und Abs. 2 DORA)</div>	Artikel 13 DORA Lernprozesse und Weiterentwicklung	Artikel 14 DORA Kommunikation <div>Kommunikationsstrategie für IKT-bezogene Vorfälle (Art. 14 Abs. 3 i.V.m. Art. 6 Abs. 8 lit. h DORA)</div> <div>Kommunikationsleitlinien für Mitarbeiter (in Bezug auf den IKT-Risikomanagementrahmen) (Art. 14 Abs. 2 DORA)</div>	Artikel 17-23 DORA <div>Richtlinien für die Behandlung IKT-bezogener Vorfälle (Art. 22 und 23 RTS RMF)</div>	Artikel 24-25 DORA <div>Leitlinien zur Priorisierung, Klassifizierung und Behebung aller während der Durchführung der Tests zutage getretenen Probleme (Art. 24 Abs. 5 DORA)</div> <div>Programm für die Tests der digitalen operationalen Resilienz (Art. 25 Abs. 1 DORA i.V.m. Art. 24 Abs. 2 DORA)</div>	Artikel 28-30 DORA <div>Strategie für das IKT-Drittparteienrisiko (Art. 28 Abs. 2 DORA)</div> <div>(optionale) Strategie zur Nutzung mehrerer IKT-Anbieter (Art. 28 Abs. 2 i.V.m. Art. 6 Abs. 9 DORA)</div> <div>Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer o. wichtiger Funktionen (Art. 28 Abs. 2 und 10 DORA; Art. 1-11 RTS TPPol)</div> <div>Leitlinie für die Nutzung von IKT-Dienstleistungen (Art. 5 Abs. 2 lit. h DORA)</div>		
Leit-/ Richtlinien																		
Weitere Dokumentationsanforderungen	<div>Bericht über die Überprüfung des IKT-Risikomanagementrahmens (Art. 6 Abs. 5 DORA i.V.m. Art. 27 RTS RMF)</div> <div>(IKT-)Revisionspläne inkl. Follow-up Verfahren bei kritischen Erkenntnissen (Art. 6 Abs. 6 und 7 i.V.m. Art. 5 Abs. 2 lit. f DORA)</div>	<div>Inventar aller IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten (Art. 8 Abs. 1 und 6 DORA)</div> <div>Inventar aller (kritischen) Informations- und IKT-Assets (Art. 8 Abs. 1, 4 und 6 DORA)</div> <div>Inventar aller Prozesse, die von IKT-Drittdienstleistern abhängen (Art. 8 Abs. 5 und 6 DORA)</div>	<div>Verfahren für das IKT-Risikomanagement (Art. 3 RTS RMF)</div> <div>Verfahren für das Management von IKT-Assets (Art. 5 RTS RMF)</div> <div>Schutzmaßnahmen für kryptografische Schlüssel (Art. 9 Abs. 4 lit. d DORA)</div> <div>Register aller Zertifikate und Zertifikatspeicher für diejenigen IKT-Assets, die kritische o. wichtige Funktionen unterstützen (Art. 7 Abs. 4 RTS RMF)</div> <div>Verfahren für das Management der IKT-Vorgänge (Betrieb) (Art. 8 RTS RMF i.V.m. Art. 9 Abs. 2 DORA)</div> <div>Verfahren für das Kapazitäts- und Leistungsmanagement (inkl. Überwachung) (Art. 9 RTS RMF i.V.m. Art. 9 Abs. 2 DORA)</div> <div>Verfahren für das Schwachstellen-Management (Art. 10 Abs. 1 und 2 RTS RMF i.V.m. Art. 9 Abs. 2 DORA)</div> <div>Verfahren für das Patch-Management (Art. 10 Abs. 3 und 4 RTS RMF i.V.m. Art. 9 Abs. 2 DORA)</div> <div>Verfahren für die Daten- und Systemsicherheit (Art. 11 RTS RMF i.V.m. Art. 9 Abs. 2 DORA)</div> <div>Verfahren, Protokolle und Tools für die Datenaufzeichnung (Logging) (Art. 12 RTS RMF)</div> <div>Verfahren, Protokolle und Tools für das Management der Netzwerksicherheit (Art. 13 RTS RMF)</div> <div>Verfahren, Protokolle und Tools zum Schutz von Informationen bei der Übermittlung (Art. 14 RTS RMF)</div> <div>Verfahren und Kontrollen für das IKT-Änderungsmanagement (Art. 9 Abs. 4 lit. e DORA; Art. 17 RTS RMF)</div> <div>Verfahren für das Identitätsmanagement (Art. 20 Abs. 1 RTS RMF)</div> <div>Verfahren für Zugangs- und Zugriffsrechte (Art. 9 Abs. 4 lit. c DORA)</div>	<div>Erkennungsmechanismen von anomalen Aktivitäten (Art. 10 DORA i.V.m. Art. 23 RTS RMF)</div> <div>IKT-Geschäftsfortführungspläne (IKT-GFP) (Art. 11 Abs. 6 lit. a DORA; Art. 24 und 25 RTS RMF)</div> <div>Dokumentation der Tests der IKT-GFP (Art. 25 Abs. 5 RTS RMF)</div> <div>IKT-Reaktions- und Wiederherstellungspläne (Art. 11 Abs. 3 DORA i.V.m. Art. 5 Abs. 2 lit. e DORA; Art. 24 u. 26 RTS RMF)</div> <div>Aufzeichnungen über die Tätigkeiten vor und während Störungen bei Aktivierung der IKT-GFP oder der IKT-Reaktions- und Wiederherstellungspläne (Art. 11 Abs. 8 DORA)</div>	<div>Verfahren für die Datensicherung (Backup) (Art. 12 Abs. 1 lit. a und Abs. 2 DORA)</div> <div>Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden (Art. 12 Abs. 1 lit. b und Abs. 2 DORA i.V.m. Art. 11 Abs. 2 lit. c DORA)</div>	<div>Programme zur Sensibilisierung für IKT-Sicherheit (Art. 13 Abs. 6 DORA i.V.m. Art. 5 Abs. 2 lit. g DORA)</div> <div>Schulungen zur digitalen operationalen Resilienz (Art. 13 Abs. 6 DORA i.V.m. Art. 5 Abs. 2 lit. g DORA)</div>	<div>Kommunikationspläne (Art. 14 Abs. 1 DORA i.V.m. Art. 11 Abs. 2 lit. e, Abs. 6 lit. b und 7 DORA; Art. 24 RTS RMF)</div> <div>Kommunikationspläne (Art. 14 Abs. 1 DORA i.V.m. Art. 11 Abs. 2 lit. e, Abs. 6 lit. b und 7 DORA; Art. 24 RTS RMF)</div>	<div>Prozess für die Behandlung IKT-bezogener Vorfälle (Art. 17 DORA i.V.m. RTS CCI; Art. 23 RTS RMF)</div> <div>Dokumentation IKT-bezogener Vorfälle und erheblicher Cyberbedrohungen (Art. 17 Abs. 2 DORA i.V.m. RTS CTIR und ITS TIR)</div>	<div>Verfahren zur Priorisierung, Klassifizierung und Behebung aller während der Durchführung der Tests zutage getretenen Probleme (Art. 24 Abs. 5 DORA)</div> <div>Validierungsmethoden (Art. 24 Abs. 5 DORA)</div>	<div>Informationsregister (Art. 28 Abs. 3 DORA i.V.m. ITS RoI)</div> <div>Ausstiegspläne (Art. 28 Abs. 8 DORA; Art. 10 RTS TPPol)</div>								

Farblégende

Strategie

Leitlinie

Richtlinie

Weiteres Dokument

Übergreifendes Dokument

Abkürzungen relevanter Rechtstexte:

DORA = Digital Operational Resilience Act (Verordnung über die digitale operationale Resilienz im Finanzsektor)
RTS = Regulatory Technical Standard (Technischer Regulierungsstandard)
ITS = Implementing Technical Standard (Technischer Durchführungsstandard)

RTS RMF = RTS ICT Risk Management Framework (IKT-Risikomanagementrahmen)
RTS CCI = RTS Classification Criteria Incidents (Klassifizierungskriterien Vorfälle)
RTS CTIR = RTS Content and Time limits Incident Reporting (Inhalt und Fristen Vorfallemeldungen)
RTS TIR = ITS Templates Incident Reporting (Vorlagen Vorfallemeldungen)
RTS TPPol = RTS ICT Third-Party Policy (IKT-Drittdienstleister-Leitlinie)
ITS RoI = ITS Register of Information (Informationsregister)

Anmerkung: Bestimmte Regelungen aus DORA, die nur für wenige Finanzunternehmen relevant sind, sind nicht Gegenstand dieser Übersicht. Nähere Informationen sind in den begleitenden Hinweisen enthalten.